Freely distributable tools for finding web vulnerabilities

Tomáš Meravý Murárik

Description

- Overview of web vulnerabilities and their classifications
- Introduction to freely available web vulnerability scanners
- Relevance of open-source tools in modern web security assessment

Project Focus

- Focus Focus areas: SQL injection, hidden file detection, outdated components
- Importance of controlled testing environments for security research

CWE-89 (SQLi)

- Typical causes: unsanitized user input concatenated into SQL, unsafe ORM usage, dynamic query building without param binding.
- Detection: injection payloads, error message analysis, blind/time-based tests.
- Impact: unauthorized data access, modification, authentication bypass.

CWE-552 (Exposed Files)

- **Typical causes: directory indexing enabled, predictable file names, deployment artifacts left on server.**
- **Detection: forced directory enumeration, public file checks, crawling for common backup/hidden file names.**
- **Impact: disclosure of secrets, config leakage, source code exposure.**

CWE-1104 (Unmaintained components)

- Typical causes: outdated dependencies, transitive libraries, lack of dependency management.
- Detection: static analysis of dependency manifests, CVE database matching.
- Impact: known exploits become trivially usable against app.

Requirements for Choosing Tools

- **Requirements for choosing tools**
  - Coverage
  - Popularity & Community Support
  - Reporting Features
  - Open-source license

Tools used

- W3af
- Nikto
- Wapiti
- Vega
- Grabber
- Dirsearch

Comparison Between General-Purpose and Specialized Tools

- **General-Purpose Tools(w3af, Nikto, Wapiti, Vega, Grabber)**
  - Broad vulnerability coverage
  - Multiple scanning modules and plugins
  - Require more configuration and time
  - Great for overall assessment and reporting
- **Specialized Tools (Dirsearch)**
  - Focused on one vulnerability type
  - Simple, fast, and efficient
  - Provide deeper, more precise results
  - Best for targeted testing and validation

Project plans

- **Tests**
- **Testing Targets**
  - Custom simple vulnerable website
  - Custom laravel website
  - DVWA

Plans for Project

- Environment setup
- Tool setup
- Optimal too configuration research